OC Support for AAA User

This chapter describes the implementation of the administrative model of *task-based authorization* used to control user access in the software system.

Table 1: Feature History

Feature Name	Release Information	Feature Description
OC support for AAA user	Cisco IOS XR Release 7.3.2	This feature allows all authorized users on XR VM to access administration data on the router through NETCONF or gRPC interface, similar to accessing the CLI. This functionality works by internally mapping the task group of the user on XR VM to a predefined group on System Admin VM. Therefore, the NETCONF and gRPC users can access the administrative information on the router even if their user profiles do not exist on System Admin VM. Command added: • aaa authorization (System Admin-VM)

OC Support for AAA User

This chapter describes the implementation of the administrative model of task-based authorization used to control user access in the software system.

Table 2: Feature History

Feature Name	Release Information	Feature Description
OC support for AAA user	Cisco IOS XR Release 7.3.2	This feature allows all authorized users on XR VM to access administration data on the router through NETCONF or gRPC interface, similar to accessing the CLI. This functionality works by internally mapping the task group of the user on XR VM to a predefined group on System Admin VM. Therefore, the NETCONF and gRPC users can access the administrative information on the router even if their user profiles do not exist on System Admin VM. Command added: • **aaa authorization (System Admin-VM)**

AAA services

AAA is part of the software base package and is available by default.

To configure authentication, authorization, and accounting (AAA) authentication at login, use the **aaa authentication login** command in global configuration mode.

A AAA service is a security framework that

- authenticates users or principals to verify their identities,
- authorizes permissions so authenticated users can perform specific tasks, and
- accounts for user and system activities by recording selected actions and sessions.

AAA (Authentication, Authorization, and Accounting) services are included by default in the software base package. Administrators can use the command set to configure user groups and task groups, ensuring that only authorized individuals have access and that all actions are tracked for regulatory or security purposes.

- Authentication commands verify the identity of users or principals.
- Authorization commands determine if authenticated users or principals are allowed to carry out specific actions.
- Accounting commands log sessions and create audit trails by recording certain user- or system-generated activities.

To configure AAA authentication at login, use the following command in global configuration mode:

```
aaa authentication login
```

Admin access methods for NETCONF and gRPC

A NETCONF/gRPC admin access method is a feature that

- enables all authorized users on the XR VM to securely access administration data on Cisco IOS XR routers using NETCONF or gRPC interfaces,
- internally maps XR VM user task groups to predefined groups on the System Admin VM, and
- allows admin access through NETCONF or gRPC even when user profiles do not exist on the System Admin VM.

NETCONF is an XML-based protocol used over Secure Shell (SSH) transport to configure and manage network devices. gRPC is an open-source remote procedure call framework that allows client applications to request information from the router and make configuration changes.

Before Cisco IOS XR Software Release 7.3.2, users who accessed administrative data through NETCONF, gRPC, or any configuration interface other than the CLI needed to belong to user groups configured directly on the System Admin VM. Otherwise, the router denied access and issued an "UNAUTHORIZED access" error. By default, XR VM only synchronized the first configured user profile to the System Admin VM. If the first user was deleted, the system synchronized the next user in the root-lr group to the System Admin VM only if no other user existed on the System Admin VM. Subsequent XR VM users were not automatically synchronized.

Beginning with Cisco IOS XR Software Release 7.3.2, the system automatically maps authorized users on XR VM to the System Admin VM based on the user's task table. This means NETCONF and gRPC users can access admin-related information on the router, even if their profiles are absent from the System Admin VM. This feature is enabled by default.

Suppose a network administrator creates several user accounts on the XR VM but does not add them explicitly to the System Admin VM. With this feature enabled, all authorized users can use NETCONF or gRPC to access administrative data on the router, streamlining operations and minimizing user account duplication across VMs.

User profile mappings between XR VM and System Admin VM

User privileges to execute commands and access data elements on the router are usually specified using certain command rules and data rules that are created and applied on the user groups.

When the internal process for AAA starts or when you create the first user, the system creates the following set of predefined groups, command rules and data rules in System Admin VM. These configurations are prepopulated to allow users of different groups (such as root-system, admin-r and aaa-r) in System Admin VM

You can use the **show running-configuration aaa** command to view the AAA configurations.

The admin CLI for the user works based on the above configurations. The root-system is the group with the highest privilege in System Admin VM. The admin-r group has only read and execute access to all data. The aaa-r group has access only to AAA data. With the introduction of the admin access feature for all users, the NETCONF and gRPC applications can also access the admin data based on the above rules and groups.

A user profile mapping is an authentication mechanism that

- establishes a direct relationship between user profiles in XR VM and System Admin VM,
- assigns user privileges based on predefined command and data rules for different user groups, and

- streamlines authentication and access control on the system.

User privileges to execute commands and access data elements on the router are defined and enforced by command and data rules assigned to user groups. When the AAA (Authentication, Authorization, and Accounting) process starts, or when you create the first user, the system automatically creates and populates a set of predefined groups, command rules, and data rules in the System Admin VM. These default group assignments, such as root-system, admin-r, and aaa-r, are designed to provide appropriate privilege levels to users in System Admin VM.

You can use the `show running-configuration aaa` command to view the AAA configurations and verify current group and rule assignments.

Example configuration

```
aaa authentication groups group aaa-r gid 100 users %%__system_user__%%
!
aaa authentication groups group admin-r gid 100 users %%__system_user__%%
!
aaa authentication groups group root-system gid 100 users "%%__system_user__%% "
!
aaa authorization cmdrules cmdrule 1 context * command * group root-system ops rx action
accept
!
aaa authorization cmdrules cmdrule 2 context * command "show running-config aaa" group aaa-r
ops rx action accept
!
aaa authorization cmdrules cmdrule 3 context * command "show tech-support aaa" group aaa-r
ops rx action accept
!
aaa authorization cmdrules cmdrule 4 context * command "show aaa" group aaa-r ops rx
action accept
!
aaa authorization cmdrules cmdrule 5 context * command show group admin-r ops rx action
accept
!
aaa authorization datarules datarule 1 namespace * context * keypath * group root-system
ops rwx action accept
!
aaa authorization datarules datarule 2 namespace * context * keypath /aaa group aaa-r ops
r action accept
!
aaa authorization datarules datarule 3 namespace * context * keypath /aaa group admin-r ops
rwx action reject
!
aaa authorization datarules datarule 4 namespace * context * keypath / group admin-r ops r
action accept
```

These key points summarize how user profile mappings and group rules affect system access and privileges:

- The admin CLI operates according to these predefined groups and their rules.
- The root-system group holds the highest privilege level within the System Admin VM.
- The admin-r group has read and execute privileges for all data, while the aaa-r group has access restricted to AAA-related data.
- With admin access available to all users, applications such as NETCONF and gRPC can also access admin data according to these group-based rules and configurations.

Administration data access rules

An administration data access rule is a security policy that

- specifies which users or groups can access administration data on a router,
- defines the permitted operations (such as read-only access) for supported management protocols like NETCONF and gRPC, and
- is implemented through command rules in the AAA authorization framework.

Administration data includes configuration and status information required for monitoring or managing routers via protocols like NETCONF and gRPC. Proper configuration of access rules ensures users can securely retrieve information without having the ability to alter device settings.

Configuration example

To grant read access to administration data for users in the `admin-r` group via NETCONF or gRPC, configure the following AAA command rule on your router:

```
Router#admin
sysadmin-vm:0_RP0#configure
sysadmin-vm:0_RP0(config)#aaa authorization cmdrules cmdrule 6
sysadmin-vm:0_RP0(config-cmdrule-6)#context netconf
sysadmin-vm:0_RP0(config-cmdrule-6)#command get
sysadmin-vm:0_RP0(config-cmdrule-6)#group admin-r
sysadmin-vm:0_RP0(config-cmdrule-6)#ops rx
sysadmin-vm:0_RP0(config-cmdrule-6)#action accept
sysadmin-vm:0_RP0(config)#commit
```

After configuration, the rule appears in the running configuration as follows:

```
aaa authorization cmdrules cmdrule 6
context netconf
command get
group admin-r
ops rx
action accept
!
```